Forcepoint

A Day in the Life of Sensitive Data

One employee. One ordinary morning. An exponential explosion of data risk. Here's how it happens and how to stop it.

The Risk Is Already Here

53%

OF INSIDER INCIDENTS ARE ACCIDENTAL OR NEGLIGENT

DTEX 2026 Cost of Insider Risks

13%

OF INCIDENTS ARE CONTAINED IN LESS THAN 30 DAYS

DTEX 2026 Cost of Insider Risks

200+ Days

AVERAGE TIME TO RESOLVE (MALICIOUS AND ACCIDENTAL) INSIDER INCIDENTS

IBM 2025 Cost of a Data Breach Report

$19.5 Million

TOTAL AVERAGE ANNUAL COST OF INSIDER INCIDENTS

DTEX 2026 Cost of Insider Risks

Meet Alice

Alice is a sales rep preparing for a high-stakes partner meeting. She's doing her job. She's not trying to cause a security incident. **Watch what happens to sensitive data as she gets ready.**

Salesforce → Excel

Alice runs a report on her top strategic accounts in Salesforce and downloads it as an Excel file. The data, includes account names, contacts and revenue figures.

Regulated PII, IP and strategic account data exits a controlled CRM environment.

Excel → Cloud

She uploads the file to a collaboration platform to share with her team. SharePoint. Box. OneDrive. It doesn't matter.

Critical data now exists in multiple locations, accessible to anyone with permission.

Excel → Public AI

Alice uses a public AI tool to summarize trends and create talking points. She uploads the Excel file directly to the prompt.

Critical data has been uploaded to Shadow AI with a risky prompt.

AI Output → Slack

She shares the AI-generated summary with her team in Slack.

New content that includes elements of critical data spreads to a collaboration channel.

Slack → External Email

Alice emails the summary to a partner outside the organization.

Critical data is exported via the riskiest channel, with no access or audit controls.

What just happened?

PII. Intellectual property. Strategic insights. In one day, all of it has now exploded across collaboration platforms, cloud storage, AI tools and external trust boundaries. Alice didn't mean to cause a problem. She was simply trying to work smarter and faster. That's what makes insider risk so hard to manage: most of it isn't malicious. It's human.

A New Approach: Security That Follows the Data

Protecting sensitive data requires a continuous approach that adapts in real time. Not a checklist. Not a set of static policies. A cycle. **Forcepoint calls this approach Data Security Everywhere.**

Discover
Establish visibility over sensitive data wherever it lives

Classify
Identify the type, business use and sensitivity level of data

Prioritize
Focus attention where risk is greatest

Protecting sensitive data isn't a checklist. **It's a continuous cycle.**

Protect
Enforce policies consistently across channels to reduce risk

Remediate
Address vulnerabilities before they become breaches

Forcepoint Data Security Cloud

All five steps connect in one unified platform: Forcepoint Data Security Cloud. One platform. One set of policies. Complete visibility across every environment where data lives, moves and is used.

Find Out More

Forcepoint